Brian Walch

From:	Michele Yorkman-Ramey
Sent:	Wednesday, June 19, 2019 1:19 PM
To:	Brian Walch
Subject:	Anonymous or hacktivism : FW: Weekly SOC Call Minutes 07-14-2016
Attachments:	HYDRA-detection strategy-1.7.pdf; HYDRA-detection strategy-2.0.pdf; Mitigation Recommendations - Cisco ROMMON - 15 JUL 2016.pdf; 16-00011000-1468509224.pdf; ATT00001.txt

-----Original Message-----
From: weeklysoc-bounces@us-cert.gov [mailto:weeklysoc-bounces@us-cert.gov] On Behalf Of Notification
Sent: Friday, July 15, 2016 2:40 PM
Subject: [Weeklysoc] Weekly SOC Call Minutes 07-14-2016

Thank you for your participation in the US-CERT Weekly SOC Call. Below are the topics that US-CERT discussed on July 14, 2016. Please keep in mind that other topics are discussed on this call as other agencies bring them up those may not appear on these minutes. If you have any topics that you would like to discuss for the next meeting, please e-mail to us at notification@us-cert.gov and we will be sure to include them on the agenda.

Meeting Minutes:

1) Follow up - ***TLP AMBER*** Hydra Report from CERT-EU regarding Compromise of Cisco Devices ***TLP AMBER***

- See attached "Recommendations to Mitigate Unauthorized Cisco ROMMON Access and Validate Boot ROMs" - Source: NSA IAD IAA U/OO/802097-16.
- See attached detection strategy reports regarding activity called Hydra involving compromise of Cisco devices (Snort rules, YARA rule and other detection strategies included).

2) Alert: Anonymous-Affiliated Actors Announce 'Day of Rage' for July 15,
- On July 9, 2016, Anonymous-affiliated actors announced physical and cyber-based protests ag ainst police brutality for a "Day of Rage" on July 15, 2016. We believe that the Day of Rag e poses a low threat of distributed denial-of- service (DDoS), data leak and defacement attacks against U.S. Government and law Enforcement websites.

Thank you,
United States Computer Emergency Readiness Team (US-CERT)
703-235-8832 / 888-282-0870
notification@us-cert.gov <mailto:notification@us-cert.gov>
Twitter: @USCERT.gov